

**Appln No. 09/892,240**

**Amdt date April 26, 2005**

**Reply to Office action of January 26, 2005**

**REMARKS/ARGUMENTS**

Claims 1-6, 8-20, 22-28, ad 40 are now pending in this application in light of the above amendments. Claims 1, 15, and 29 have been amended. Claims 7, 21, and 29-39 have been cancelled. Claim 40 has been added. The amendments find full support in the original specification, claims, and drawings. No new matter has been added. In view of the above amendments and remarks that follow, reconsideration, reexamination, and an early indication of allowance of the now pending claims 1-6, 8-20, 22-28, and 40 are respectfully requested.

The Examiner objects to the specification due to certain informalities. Amendments to the specification have been made on pages 5, 13, and 21 to overcome the Examiner's objection. The amendments do not add any new matter. Entry of the amendments to the specification is respectfully requested.

Claims 1, 4, 7, 15, 18, 21, 29, and 33-35 are rejected under 35 U.S.C. 112, second paragraph, because some claim limitations have insufficient antecedent basis. The amendments to the claims overcome this rejection. Withdrawal of the rejection under 35 U.S.C. 112, second paragraph, is respectfully requested.

Claims 29 and 38 are rejected under 35 U.S.C. 102(b) as being anticipated by Buer (U.S. Patent No. 5,697,284). Claims 30-37 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over one or more of Buer, Guski et al. (U.S. Patent No. 5,661,807), Windirsch (U.S. Patent No. 6,760,439), Pawlowski (U.S. Patent No. 5,469,547), and Kanda (U.S. Patent No. 6,769,063).

**Appln No. 09/892,240**  
**Amdt date April 26, 2005**  
**Reply to Office action of January 26, 2005**

Claims 29-39 have now been canceled without prejudice for pursuing in a continuation application. Withdrawal of the rejection is therefore respectfully requested.

Claims 1-3, 5-17, and 19-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanda et al. (U.S. Patent No. 6,769,063) in view of Callum (U.S. Patent No. 6,320,964) and Windirsch (U.S. Patent No. 6,760,439). Claims 4 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanda et al. in view of Callum, Windirsch, and Steinman et al. (U.S. Patent No. 6,591, 349). Applicant respectfully traverses these rejections.

Independent claims 1 and 15 have now been amended to include a "two-level multiplexer circuitry including a multiplexer on a first level coupled to a multiplexer on a second level, wherein the two-level multiplexer circuitry avoids swapping of data loaded from a previous round of cryptographic processing without incurring an extra clock cycle." None of the cited references teach or suggest such a two-level multiplexer circuitry.

Although Windirsch discloses a device for implementing a block-ciphering process that includes various multiplexers, Windirsch fails to disclose the recited two-level multiplexer circuitry that " avoids swapping of data loaded from a previous round of cryptographic processing without incurring an extra clock cycle." Accordingly, claims 1 and 15 are now in condition for allowance.

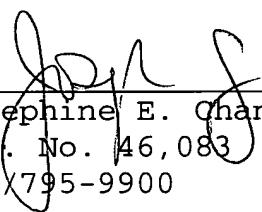
**Appln No. 09/892,240**  
**Amdt date April 26, 2005**  
**Reply to Office action of January 26, 2005**

Claims 2-14 and 16-28 are also in condition for allowance because they depend on an allowable base claim, and for the additional limitations contained therein.

Claim 40 is new in this application. Claim 40 is also in condition for allowance because it depends on an allowable base claim. In addition, claim 40 further adds the limitation that "the multiplexer on the first level loads the data block in response to a first signal value, and further loads data from a previous round of cryptographic processing in response to a second signal value, and the multiplexer on the second level swaps the loaded data from the previous round of cryptographic processing in response to a third signal value, and further fails to swap the loaded data from the previous round of cryptographic processing in response to a fourth signal value." None of the cited references teach or suggest this limitation.

In view of the above amendments and remarks, Applicant respectfully requests reconsideration, reexamination, and an early indication of allowance of the now pending claims 1-6, 8-20, 22-28, and 40.

Respectfully submitted,  
CHRISTIE, PARKER & HALE, LLP

By   
Josephine E. Chang  
Reg. No. 46,083  
626/795-9900

JEC/lal  
LAL PAS607773.3--\*-04/26/05 4:15 PM